

Eavesdropping in Semiquantum Key Distribution Protocol: Classical vs. Hadamard Bob

Arpita Maitra* and Goutam Paul#

*Applied Statistics Unit, Indian Statistical Institute, 203 B T Road,
Kolkata 700 108, India, Email: arpita76b@rediffmail.com

#Department of Computer Science and Engineering, Jadavpur University,
Kolkata 700 032, India, Email: goutam.paul@ieee.org

The quantum key distribution protocol with classical Bob, well known as semiquantum key distribution, has been proposed a few years back (Boyer et al., PRL 2007, PRA 2009). In this protocol Alice has the same capability as in the traditional BB84 protocol, but Bob is limited by the constraint that he can measure or prepare qubits only in $\{|0\rangle, |1\rangle\}$ basis and reflect any other qubit (or in other words, let it go undisturbed). In this scheme the qubits travel from Alice to Bob and then again from Bob to Alice. We study an eavesdropping strategy on this scheme that listens to the channel in both the directions. With the same level of disturbance induced in the channel, Eve can be extract more information using our two-way strategy than what can be obtained by the direct application of one-way eavesdropping in case of BB84 protocol. Towards resisting this eavesdropping strategy, we modify the semiquantum scheme by incorporating a Hadamard gate at Bob's end.

Keywords: BB84 Protocol, Binary Symmetric Channel, Hadamard Gate, Key Pre-Distribution, Optimal Eavesdropping, Quantum Cryptography, Semiquantum.

I. INTRODUCTION

The BB84 protocol is used by Alice and Bob to settle on a secret classical bit-string over an insecure quantum channel where Eve can have access. The basic idea behind the security of the famous BB84 [1] protocol is that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s). There are a number of important papers that analyze this scheme and we refer to [3, 6, 7] and the references therein for further reading. The BB84 protocol [1] uses the bases $|0\rangle, |1\rangle$ and $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. In this case, Bob has the capability of measuring the qubits in either Z , i.e., $\{|0\rangle, |1\rangle\}$ or X , i.e., $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ basis.

In [4], it has been considered that Bob does have limited capability and he can do the following.

- Whenever a qubit passes through Bob, he can let it go undisturbed, or in other words he can reflect the qubit to Alice (CTRL bits).
- Otherwise
 - he can measure the qubit in the Z basis and
 - prepare a fresh qubit in the same basis and send it to Alice (SIFT bits).

Based on this limited capability of Bob, semiquantum key distribution has been presented in [4] and later it has been analyzed in more detail in [5]. The authors call the Z basis as the classical basis, as it has one-to-one correspondence with the classical bits. Bob is called

classical since he prepares and measures qubits in this basis only. Alice is not classical, as she needs to deal with quantum superposition of the computational basis states. Thus the protocol is called *semiquantum*. We give a brief description of the protocol [4] in Table I.

In [4, 5], the authors proved that the protocol is robust. This is in the sense that for any attack inducing no error on TEST and CTRL bits, Eve's final state is independent of the qubits chosen by Bob as SIFT and the states sent by Alice. However, they did not give any quantitative estimate connecting the disturbance experienced by Alice and the information leakage at Eve's end. In [5, Section I], the authors made the following comment:

Note that our result does not imply that Eve cannot gain a large amount of information by inducing a very small but nonzero noise on qubits. It is however our belief that such a discontinuity of "information versus disturbance" does not occur, but the question is beyond the scope of this paper and is left for future research.

This gives us motivation to investigate the exact relationship between the disturbance and information leakage under certain eavesdropping model. In the semiquantum protocol [4], the qubits need to travel in two directions and thus the eavesdropper has the advantage to look into the qubits twice instead of once as in the case of BB84 [1]. In this paper, we analyze the security of the semiquantum protocol in the light of symmetric incoherent eavesdropping strategy of [7] that has already been studied on BB84 protocol. Since Eve's goal is to decide the secret key bits established between Alice and Bob, we take the success probability of Eve in guessing the key bits correctly as a security parameter.

There could be different attack models and the security analysis in one model may widely differ from that in another model. However, to the best of our knowledge, no quantitative study has been attempted yet in the

1. Alice generates $N = 8n(1 + \delta)$ many qubits randomly in Z basis or X basis.
2. For each qubit received at Bob's end, he chooses randomly
 - either to reflect it (CTRL)
 - or to measure it in Z basis and resend it in the same state he measured (SIFT).
3. Alice measures each qubit in the basis she sent.
4. Alice publishes which are the Z bits she sent and Bob publishes which ones he chose to SIFT^a.
5. Alice checks the error-rate in the CTRL bits and aborts the protocol if the error-rate in either of the basis is more than some predefined threshold value.
6. Alice randomly chooses n SIFT bits as TEST bits and publishes them.
7. Bob publishes the values of these TEST bits.
8. Alice checks the error rate in these bits and aborts if the error-rate is more than some predefined value.
9. Alice and Bob select the first n remaining SIFT bits to be used as INFO bits.
10. Alice publishes ECC and PA data and then she and Bob use them to extract the final m -bit secret key from n -bit INFO string.

^aThus after this step, the intersection of these two sets, is known to both of them and hence it is known to them when Alice transmitted the Z -basis and Bob chose to SIFT. There are approximately $\frac{N}{4} \geq 2n$ such bits from which the secret key will ultimately be chosen.

TABLE I: Semiquantum Key Distribution with Classical Bob

context of semiquantum key distribution when non-zero disturbance is introduced by the eavesdropper. Hence, we investigate this eavesdropping strategy exploiting the model of [7]. Our study shows that the two-way application of symmetric incoherent eavesdropping strategy helps in obtaining more information in the semiquantum protocol [4] than that can be obtained by using one-way eavesdropping as applicable on the BB84 [1] under this model.

In Section II, we give a brief review of the attack model and the prerequisites for our current work. In Section III, we propose a two-way eavesdropping strategy for the semiquantum protocol and show that the eavesdropper can increase her advantage by combining suitably her observations in both the directions of communication. Finally, in Section IV, we propose a better resistance to our attack by applying Hadamard gate at Bob's end in the semiquantum protocol.

II. BACKGROUND

In this paper, we consider the same symmetric incoherent optimal eavesdropping model of [7] that was used for the traditional BB84 protocol [1]. It is symmetric, because there will be equal error probability at Bob's end corresponding to different bases and it is incoherent as Eve works with each individual qubit.

In general, Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a four dimensional probe $|W\rangle$ of two qubits (as in [7, Section III]) that interacts unitarily with $|\mu\rangle$. Eve's measurement is delayed till Alice announces the basis that has been used (i.e., by that time Bob has already measured the state).

We can model it as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$, where U is the unitary operator and after its application, $|\tau\rangle$ is the entangled state of the qubit that Alice sent to Bob and the probe applied by Eve. Let D be the disturbance in the channel due to the interaction by Eve and $F = 1 - D$ be the fidelity. For the $|0\rangle, |1\rangle$ basis, i.e., the Z basis, one can write the eavesdropping interaction as

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{F}|E_{00}\rangle|0\rangle + \sqrt{D}|E_{01}\rangle|1\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{D}|E_{10}\rangle|0\rangle + \sqrt{F}|E_{11}\rangle|1\rangle. \end{aligned} \quad (1)$$

Similar equations can be written for the X basis. In the traditional BB84 protocol [1], Alice encodes the 0 bit by $|0\rangle$ or $|+\rangle$ and the 1 bit by $|1\rangle$ or $|-\rangle$. After Bob completes the measurement and Alice and Bob publish relevant information over insecure channel, Eve measures the probes she has applied to obtain information about the secret bits. Following the analysis in [6, 7], it can be shown that with the optimal eavesdropping strategy, Eve's average success probability in correctly guessing a secret bit is

$$P_E^{(1)}(D) = \frac{1}{2} + \sqrt{D(1-D)}. \quad (2)$$

Since the *advantage* of the eavesdropper can be defined as the amount by which the success probability exceeds the probability of random guessing (which, in this case, is $\frac{1}{2}$), the advantage is given by $A_E^{(1)}(D) = \sqrt{D(1-D)}$.

Note that the strategy of [7] can directly be used towards eavesdropping against the semiquantum protocol [4]. Eve will try to interact during the communication from Alice to Bob inducing a disturbance D and thus the success probability of Eve will be what mentioned in (2) above. However, we like to explore beyond this trivial application of the eavesdropping strategy of [7] on BB84 protocol [1] in semiquantum protocol [4]. Towards this, we consider that the eavesdropper will try to extract information during the transmission of qubits both from Alice to Bob and Bob to Alice. This is explained in the next section in detail.

III. ANALYSIS OF THE SEMIQUANTUM PROTOCOL: TWO-WAY EAVESDROPPING

When Alice sends a qubit $|\mu\rangle$ to Bob, Eve lets a probe $|W\rangle$ that interacts unitarily with $|\mu\rangle$. Thus the interaction can be modelled as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$. If Bob performs a measurement, then the 3-qubit entangled state $|\tau\rangle$ collapses to a 3-qubit post-measurement product state $|\tau_m\rangle$. When the corresponding qubit (either reflected or measured and resent) returns from Bob to Alice, then again Eve tries to interact with a probe $|W'\rangle$ and the unitary operation can be written as $U'(|\tau''\rangle, |W'\rangle) = |\tau'\rangle$, where $|\tau''\rangle$ is $|\tau\rangle$ or $|\tau_m\rangle$, according as Bob reflects or measures (respectively), and $|\tau'\rangle$ is a 5-qubit state. Eve's measurement is delayed till Alice and Bob announce the public information and the measurements at Alice's side are finished. Measurements at Bob's side get finished even earlier during the intermediate stage. Eve will try to cleverly use the information obtained from both the cases. In particular, if the outcomes of eavesdropping in both the directions match, then indeed that is correct with a higher probability.

A. The Binary Symmetric Channel Model

One may refer to [7] to note that the analysis can be done considering the model of Binary Symmetric Channel (BSC). The main question here is whether more information can be extracted at Eve's end by looking into both the directions of qubit transmission rather than just interacting during one side as in BB84. Eve's advantage in obtaining the information in these two cases need to be compared against the same disturbance induced in the communication channels. Consider the case when both the channels are analyzed, one while qubits move from Alice to Bob and another during the movement from Bob to Alice. Now there are two scenarios.

- Qubits that Bob measures and then prepares and resends (SIFT bits).
- Qubits that are reflected (CTRL bits).

For both the scenarios, we have two consecutive Binary Symmetric Channels (BSCs) with error probability p in each one due to eavesdropping. (There can be eavesdropping inducing different error probabilities p_1, p_2 in the two channels, and that can be taken care of in a similar manner.) Following Equation 1, we can write for the channel between Alice and Bob

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{p}|E_{10}\rangle|0\rangle + \sqrt{1-p}|E_{11}\rangle|1\rangle, \end{aligned} \quad (3)$$

where W is the initial state of the pair of qubits at Eve's hand.

Lemma 1 *For the SIFT bits, the round trip channel from Alice to Bob and back to Alice is equivalent to a binary symmetric channel with error probability $2p(1-p)$.*

Proof : Since Bob is performing measurement after Eve's interaction represented by Equation (3), the communication from Alice to Bob and that from Bob to Alice happen through two separate binary symmetric channels with the same error probability p cascaded to each other, as shown in Figure 1. The first BSC corresponds to the transmission from Alice to Bob and the second one corresponds to the transmission from Bob to Alice.

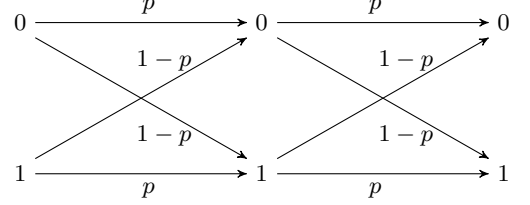


FIG. 1: Cascaded BSC model for the SIFT bits

Consider one round-trip communication from Alice to Bob and then back to Alice. If Alice sends 0, the error-path is either $0 \rightarrow 0 \rightarrow 1$ or $0 \rightarrow 1 \rightarrow 1$. The path is symmetric when Alice sends 1. Thus, the error-probability would be given by

$$\begin{aligned} &P(\text{no error: Alice} \rightarrow \text{Bob}) \cdot P(\text{error: Bob} \rightarrow \text{Alice}) \\ &+ P(\text{error: Alice} \rightarrow \text{Bob}) \cdot P(\text{no error: Bob} \rightarrow \text{Alice}) \\ &= (1-p)p + p(1-p) = 2p(1-p). \end{aligned}$$

■

Lemma 2 *For the CTRL bits, the round trip channel from Alice to Bob to Alice is equivalent to a binary symmetric channel with error probability $2p(1-p)$.*

Proof : Without loss of generality, let us consider when Alice sends 0. The case when Alice sends 1 would be symmetric.

According to Equation (3), Bob will receive a qubit entangled with the two bits of Eve, having the three-qubit entangled state $\sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle$. Bob will send the entangled qubit received as it is to Alice. Let W' be the initial state of the new pair of qubits at Eves hand with which she will interact unitarily with the qubit sent from Bob to Alice. This interaction can be written as

$$\begin{aligned} &I \otimes U(\sqrt{1-p}|E_{00}\rangle|0\rangle + \sqrt{p}|E_{01}\rangle|1\rangle, |W'\rangle) \\ &= \left((1-p)|E_{00}\rangle|E'_{00}\rangle + p|E_{01}\rangle|E'_{10}\rangle \right) |0\rangle \\ &\quad + \sqrt{p(1-p)} \left(|E_{00}\rangle|E'_{01}\rangle + |E_{01}\rangle|E'_{11}\rangle \right) |1\rangle, \end{aligned}$$

where E'_{ij} 's are the new two-qubit probes at Eve's hand corresponding to Bob sending bit i and Alice receiving bit j . Thus, the probability that Alice measures 0 is $(1-p)^2 + p^2$ and that she measures 1 is $2p(1-p)$. ■

We need to be explicit about Lemma 1 and Lemma 2 as the situation in both these cases are different. In one

case (SIFT) the qubit is measured at Bob's end and then a newly created qubit is sent, i.e., one qubit moves from Alice to Bob and a corresponding different one moves from Bob to Alice back. In the other case, the qubit is just reflected (CTRL), i.e., it is the same qubit that is travelling in both the directions (Alice to Bob and Bob to Alice). It is important to note that the error in the channel observed by Alice is the same in both the cases (CTRL and SIFT). This is the reason, the eavesdropping model of [7] remains symmetric even when it is applied to the semiquantum protocol in both the directions.

Combining Lemma 1 and Lemma 2, we can write the following Theorem.

Theorem 1 *The round trip channels from Alice to Bob to Alice when Bob measures and sends a fresh qubit (SIFT) and when he just reflects the received qubit (CTRL) are equivalent, and both act as a binary symmetric channel with error probability $2p(1-p)$.*

Let $D_{one-way}$ and $D_{two-way}$ be the disturbances in the one-way BB84 protocol and the two-way semiquantum protocol respectively. We take $D_{one-way} = D$ and we have shown that $D_{two-way} = 2p(1-p)$. Both the attacks should be compared in the same footing, i.e., Eve's advantages have to be compared at the same disturbance values. For this reason, we take $D_{two-way} = D_{one-way}$, i.e., $D = 2p(1-p)$.

In the last section, we have noted that for optimal eavesdropping [7] in BB84 protocol, the probability of correct guess by Eve can be expressed as $P_E^{(1)}(D) = \frac{1}{2} + \sqrt{D(1-D)}$. That is, inducing a disturbance $D \in [0, 0.5]$ in the channel (that can be observed at Bob's end), Eve can guess the secret bit with a probability $\frac{1}{2} + \sqrt{D(1-D)}$.

We now use the same strategy as in [7] where Eve will interact with the qubit transmitted from Alice to Bob and the corresponding qubit from Bob to Alice. The disturbance induced in each of those cases will be p (the error probability of BSC) and the value of p will be such that $D = 2p(1-p)$. That is, in the semiquantum protocol, when Alice measures the qubits finally returned to her, she will experience the error probability D . We denote the probability of correct guess by Eve by $P_E^{(2)}(D)$ and present the detailed analysis below.

B. Detailed Analysis of Two-way Eavesdropping

Eve will have two guesses for the forward and backward communication. In each guess, following (2) (see also [7]), Eve has the success probability $p_E = \frac{1}{2} + \sqrt{p(1-p)} = \frac{1}{2} + \epsilon$, where $\epsilon = \sqrt{p(1-p)}$. If both the guesses give the same outcome, then the probability that the bit guessed is correct increases. Suppose during the forward communication from Alice to Bob, Eve has a success probability of $\frac{1}{2} + \epsilon_1$ and during the backward communication from Bob to Alice, Eve has a success probability of $\frac{1}{2} + \epsilon_2$.

For a particular bit, let $P_E^{(2,match)}(D)$ be Eve's posterior probability that the bit sent was b , when both her forward and the backward guesses give the same outcome $b \in \{0, 1\}$. The following result is easy to show.

Proposition 1 $P_E^{(2,match)} = \frac{1}{2} + \frac{\epsilon_1 + \epsilon_2}{1 + 4\epsilon_1\epsilon_2}$.

The above expression is a simplified form of $\frac{(\frac{1}{2} + \epsilon_1)(\frac{1}{2} + \epsilon_2)}{(\frac{1}{2} + \epsilon_1)(\frac{1}{2} + \epsilon_2) + (\frac{1}{2} - \epsilon_1)(\frac{1}{2} - \epsilon_2)}$. Note that $\frac{1}{2} + \frac{\epsilon_1 + \epsilon_2}{1 + 4\epsilon_1\epsilon_2} \geq \frac{1}{2} + \epsilon_1$, if and only if $\epsilon_1 \leq \frac{1}{2}$. Similar conclusion holds for ϵ_2 as well. This implies that Eve's success probability increases, when she observes the same outcome b in both directions and guesses that indeed b was sent.

Let us now substitute $\epsilon_1 = \epsilon_2 = \sqrt{p(1-p)}$, where $2p(1-p) = D$. When Eve observes the same outcome in both the directions, let her success probability as a function of the disturbance be denoted by $P_E^{(2,match)}(D)$. Thus, we have the following result.

Lemma 3 $P_E^{(2,match)}(D) = \frac{1}{2} + \frac{\sqrt{D/2}}{\frac{1}{2} + D}$.

The corresponding advantage is given by $A_E^{(2,match)}(D) = \frac{\sqrt{D/2}}{\frac{1}{2} + D}$.

One may easily check that $\frac{\sqrt{D/2}}{\frac{1}{2} + D} \geq \sqrt{D(1-D)}$ for $D \in [0, \frac{1}{2}]$ and in this case, Eve's advantage for the semiquantum protocol is better than what is achieved in the eavesdropping [7] in BB84 protocol.

When both the cases do not have the same outcome, then the situation is not encouraging. In this case one has to consider one of the two outcomes as the correct guess. Without loss of generality, we accept the outcome of the first observation as the correct guess. In this case,

$$P_E^{(2,mismatch)}(D) = \frac{1}{2} + \sqrt{p(1-p)} = \frac{1}{2} + \sqrt{D/2}. \quad (4)$$

It is immediate to note that $\sqrt{D/2} \leq \sqrt{D(1-D)}$ for $D \in [0, \frac{1}{2}]$ and in this case Eve suffers with the decreased advantage.

Thus while calculating the average advantage, we consider the following strategy: "if the outcomes observed by Eve in both the directions are the same bit b , she guesses b , else she discards her guess in the backward direction and considers only the guess during the forward direction." Let $P_E^{(2,avg)}(D)$ denote Eve's average success probability when she follows the above strategy.

Theorem 2 $P_E^{(2,avg)}(D) = \frac{1}{2} + \frac{\sqrt{D/2}(3+2D)}{2(1+2D)}$.

Proof : It is clear that both the match and the mismatch happens with probability $\frac{1}{2}$. Hence the average success probability of Eve is given by

$$P_E^{(2,avg)}(D) = \frac{1}{2}P_E^{(2,match)}(D) + \frac{1}{2}P_E^{(2,mismatch)}(D).$$

Substituting values of the probabilities from Lemma 3 and Equation (4), we get the result. ■

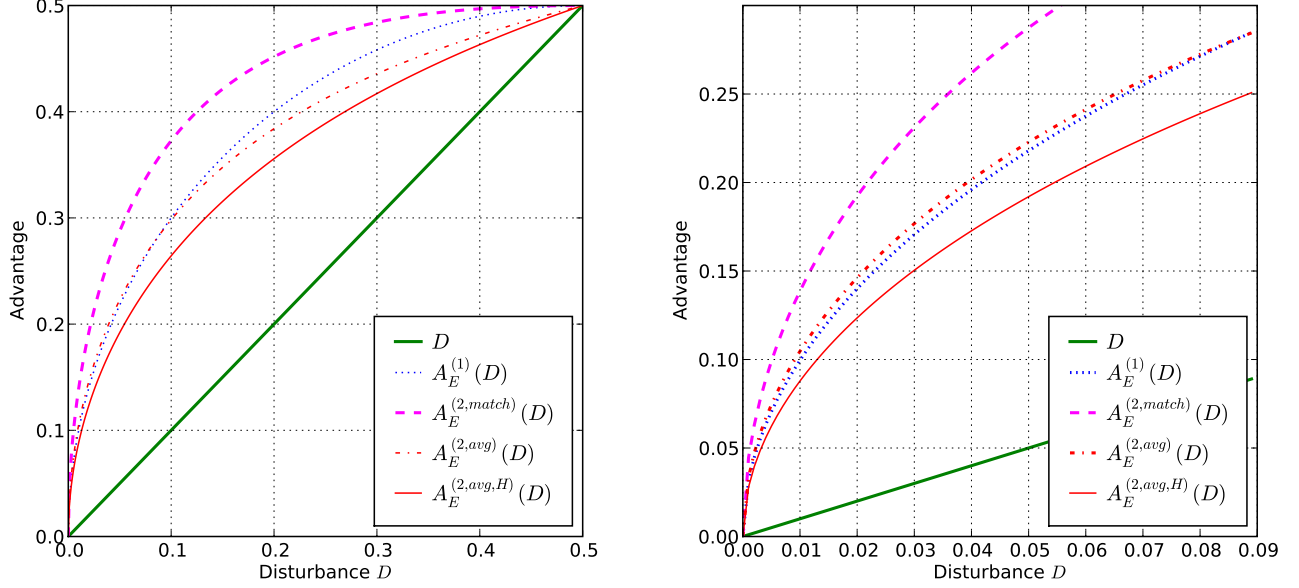


FIG. 2: Advantage of the eavesdropper as a function of disturbance D under different attack models (magnified portion for $0 \leq D \leq 0.09$ is shown on the right).

The average advantage is given by

$$A_E^{(2,avg)}(D) = \frac{\sqrt{D/2}(3+2D)}{2(1+2D)}.$$

In Figure 2, we plot the advantages for different attack strategies versus D . Note that $P_E^{(2,avg)}(D) > P_E^{(1)}(D)$, i.e., Eve has more advantage in the semiquantum protocol, if $D < 0.0877$ (upto the fourth decimal place). This region is shown magnified in the right portion of Fig. 2 for a clearer pictorial exposition.

The summarized strategy of eavesdropping on the semiquantum protocol is shown in Table II.

This provides more information to the eavesdropper in certain range in the semiquantum protocol [4] than in BB84 [1] and thus our two-way eavesdropping on the the semiquantum protocol recovers more information than what can be obtained using the idea of [7] directly as it was applied against BB84.

For the semiquantum protocol, Eve does not care to have any information about the CTRL bits as those bits are not used in generating the final secret key. A priori, Eve does not have any information which are CTRL and which are SIFT bits and thus she needs to probe all the bits, with the constraint that the error introduced in the channel should be the same in both the cases. This is guaranteed following Lemma 1, Lemma 2 and Theorem 1.

The incoherent eavesdropping model of [7] can be applied for the SIFT bits immediately due to the reason that those bits are measured and then freshly prepared at Bob's end. Thus the eavesdropping by two unitary interactions in the two different channels (Alice to Bob

<ol style="list-style-type: none"> 1. For $D \geq 0.0877$, apply unitary interaction for eavesdropping only during the communication between Alice and Bob (same as BB84). 2. For $D < 0.0877$, apply unitary interaction during both the communications (Alice to Bob and Bob to Alice) with disturbance in each channel p, where $D = 2p(1-p)$.
<ol style="list-style-type: none"> (a) If the bits obtained through the two different interactions are same, then accept that as the guessed bit. (b) If the bits obtained through the two different interactions are different, then accept the bit obtained during the communication from Alice to Bob as the guessed one.

TABLE II: Eavesdropping strategy on the semiquantum protocol of [4] with classical Bob.

and Bob to Alice) are on two different (but corresponding) qubits that represent the same bit information in the semiquantum protocol. We consider the advantage of our two-way idea comparing to the eavesdropping strategy of [7] that had been applied as it was done against BB84. In our case, when the observation from the two interactions are same, the success probability of guessing that bit improves significantly for any $D \in [0, 0.5]$. When it is not, the success probability decreases for any $D \in [0, 0.5]$, but on an average case it is better for certain

range of D as described above.

IV. USING HADAMARD GATE AT BOB'S END

In Table III, we present our new algorithm with Hadamard Bob. The main motivation here is to add further security for the SIFT bits (as explained in Step 7) which will actually be used to prepare the secret key. The random application of Hadamard gate on these bits will not allow Eve to guess those bits during the communication from Bob to Alice. We emphasize that Alice only

- 1*. Alice generates $N = 8n(1 + \delta)$ many qubits randomly in Z basis or X basis.
2. For each qubit received at Bob's end, he chooses randomly
 - (i) either to reflect it (CTRL)
 - (ii) or to measure it in Z basis and resend it "in the same state or applying the Hadamard gate" based on the outcome of an unbiased coin tossing on what he measured (SIFT).
3. Alice will store the received qubits in quantum memory. (*No measurement will be done at this point.*)
- 4*. Alice publishes which are the Z bits she sent and Bob publishes which ones he chose to SIFT.
5. Alice measures the CTRL bits. Then she checks the error-rate in the CTRL bits and aborts the protocol if the error-rate in either of the basis is more than some predefined threshold value. (*This is the first point when Alice measures.*)
- 6*. Alice randomly chooses n SIFT bits as TEST bits and publishes them.
7. Bob publishes the values of these TEST bits and also where he has used Hadamard gate.
8. Alice then measures these qubits in corresponding basis and then checks the error rate in these bits and aborts if the error-rate is more than some predefined value. (*This is the second point when Alice measures*)^a.
- 9*. Alice and Bob select the first n remaining SIFT bits to be used as INFO bits.
- 10*. Alice publishes ECC and PA data and then she and Bob use them to extract the final m -bit secret key from n -bit INFO string.

^aShe measures either in Z basis, when Bob has not applied the Hadamard gate or in X basis, when Bob has applied the Hadamard gate.

TABLE III: Semiquantum Key Distribution with Hadamard Bob. The * marked steps are the same as in the semiquantum protocol of [4] with Classical Bob.

measures some portion of the SIFT bits (TEST bits) for checking the error in the channel. However, she does not

need to measure the rest of the SIFT bits where from the INFO bits are chosen, because she herself had generated these bits. Our Hadamard Bob exploits this feature of the semiquantum protocol to confuse Eve. All these bits come in $\{|0\rangle, |1\rangle\}$ to Bob from Alice and consider that Eve interferes during this stage. However, at the time of resending (as explained in Step 2(ii) of Table III), these are randomly transferred to $\{|+\rangle, |-\rangle\}$ basis in half of the cases. Eve cannot have any prior or posterior information where the Hadamard gate is used during the resend by Bob as Bob will never publish that. Thus, if Eve tries to guess the basis randomly during the backward communication from Bob to Alice, then her success probability would be $\frac{1}{2}$ only. In Proposition 1, substituting $\epsilon_2 = 0$, we have the success probability as $\frac{1}{2} + \epsilon_1 = \frac{1}{2} + \sqrt{D/2}$. Hence, Eve has some advantage over random guessing only during the forward communication and it seems that she learns nothing during the backward communication.

Instead of randomly guessing the basis, she can choose to measure in the Z -basis all the time. Then for the resend bits, she would have advantage ϵ_2 half of the times and advantage 0 the rest of the times. So her average success probability for the backward phase would be

$$P_E^{(2,bk,H)}(D) = \frac{1}{2} \left(\frac{1}{2} + \epsilon_2 \right) + \frac{1}{2} \left(\frac{1}{2} \right) = \frac{1}{2} + \frac{\epsilon_2}{2},$$

where $\epsilon_2 = \sqrt{p(1-p)}$. In this case, during the backward communication, she learns something, but this information is less than that she would have learned for the two-way eavesdropping strategy on the semiquantum protocol with classical Bob [4]. Replacing ϵ_2 by $\frac{\epsilon_2}{2}$ in Proposition 1, we have

$$P_E^{(2,match,H)}(D) = \frac{1}{2} + \frac{3\sqrt{\frac{D}{2}}}{2+2D}.$$

Hence the average success probability of Eve is given by

$$\begin{aligned} P_E^{(2,avg,H)}(D) &= \frac{1}{2} P_E^{(2,match,H)}(D) + \frac{1}{2} P_E^{(2,mismatch)}(D) \\ &= \frac{1}{2} + \sqrt{D/2} \left(\frac{5+2D}{4+4D} \right). \end{aligned}$$

This is less than $P_E^{(2,avg)}(D)$. Obviously, the corresponding advantage

$$A_E^{(2,avg,H)} = \sqrt{D/2} \left(\frac{5+2D}{4+4D} \right)$$

is less than $A_E^{(2,avg)}$. One may refer to Figure 2 for a graphical comparison. Thus, given the eavesdropping strategy discussed above, our strategy of semiquantum key distribution with Hadamard Bob is more secure than that with classical Bob as in [4].

Also it may be checked that $P_E^{(2,avg,H)}(D)$ is less than $\frac{1}{2} + \sqrt{D(1-D)}$ for any $D \in [0, 0.5]$. Thus, the attacker does not need to go for the two-way eavesdropping in this

case inducing error probability p such that $D = 2p(1-p)$. Instead, eavesdropping in the channel from Alice to Bob inducing error probability D will provide better success probability for Eve which is the same attack as described in [7]. Thus, in this respect, one can say that against our semiquantum key distribution strategy with Hadamard Bob, the best attack known so far is the one described in [7] and the two-way eavesdropping does not provide any additional advantage.

V. CONCLUSION

Boyer et al. (PRL 2007, PRA 2009) introduced the quantum key distribution protocol with classical Bob, where Bob can measure or prepare qubits only in $\{|0\rangle, |1\rangle\}$ basis and reflect any other qubits. They showed the robustness of the protocol, but left open any analysis regarding how the amount of information leakage to the eavesdropper is related to the disturbance caused by

her. This is the motivation behind our current work. We analyzed an eavesdropping strategy on this scheme and explicitly derived eavesdropper's advantage as a function of the disturbance. Here our investigation exploits the model of [7] in both the directions of communication (Alice to Bob and Bob to Alice). Our two-way eavesdropping strategy against the semiquantum protocol extracts more information on the secret bits than that could be obtained by direct one-way application of the strategy in [7] that worked on BB84.

We also proposed a variant of the scheme by Boyer et al., where we replace the classical Bob by a Hadamard Bob, i.e., for the resend bits, he randomly applies the Hadamard gate in half of the cases, and the rest he resends as it is. We show that this semiquantum key distribution with Hadamard Bob is more secure than that with classical Bob. The two-way eavesdropping that we have proposed in case of semiquantum protocol with classical Bob [4] does not succeed after introducing the Hadamard gate.

-
- [1] C. H. Bennett and G. Brassard. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).
 - [2] E. Biham and T. Mor. Physical Review Letters, 79, 4034–4037 (1997).
 - [3] D. Bruß. Physical Review Letters, 81, 3018–3021 (1998) [quant-ph/9805019].
 - [4] M. Boyer, D. Kenigsberg and T. Mor. Physical Review Letters, 99, 140501 (2007).
 - [5] M. Boyer, R. Gelles, D. Kenigsberg and T. Mor. Physical Review A, 79(3), 032341 (2009).
 - [6] J. I. Cirac and N. Gisin. Physics Letters A, 229(1), 1–7 (1997) [quant-ph/9702002].
 - [7] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. -S. Niu, and A. Peres. Physical Review A, 56(2), 1163–1172 (1997).
 - [8] S. J. D. Phoenix. Physical Review A, 48(1), 96–102 (1993).
 - [9] S. Wiesner. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.